AN INTEROPERABILITY ROAD MAP FOR C4ISR LEGACY SYSTEMS

LTC John A. Hamilton, Jr., USA, Capt Jerome D. Rosen, USAF, and Maj Paul A. Summers, USAF

Modern military operations require interoperability. The Department of Defense (DoD) has made tremendous interoperability gains over the last few years. Unfortunately, without a way to assess the status of interoperability throughout the department, it is difficult to quantify this progress. Although interoperability issues are persistent and visible, the number of interoperability successes is easily overlooked. Most systems developed today meet the interoperability requirements that were specified in their operational requirements documents (ORDs). The application of a set of metrics addressing this domain would shed more light on the situation and highlight the successes of the many agencies that have labored to produce interoperable systems. Effective metrics would enable the services and agencies to make informed decisions about the allocation of scarce resources to solve interoperability in already fielded systems.

The pejorative use of the term "legacy system" often occurs when communications and computer systems are described. This is unfortunate because many fielded systems are performing well and meeting or exceeding their original specifications.

"C4ISR" refers to systems that are part of the Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance domain. The C4ISR domain is one of four domains for which the Joint Technical Architecture specifies a domain annex. C4ISR is defined in the Joint Technical Architecture (JTA; Defense Information Systems Agency, 1999) as those systems that

- support properly designated commanders in the exercise of authority and direction over assigned and attached forces across the range of military operations;
- collect, process, integrate, analyze, evaluate, or interpret available information concerning foreign countries or areas;

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Interoperability Road Map for C4ISR Legacy Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space & Naval Warfare Systems Comd,Joint Forces Program Office,San Diego,CA,92152**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Acquisition Review Quarterly, Winter 2002

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

- systematically observe aerospace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means; and

- obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

The JTA specifies a minimal subset of interoperability requirements. It is becoming trite to say that the JTA is necessary but not sufficient to achieve interoperability. Interoperability is a hot-button issue and it certainly should be. However, as Col. Thomas Andrew, U.S. Air Force, has observed, "There is a lot of interoperability out there. Many C4ISR systems do interoperate quite well together." As the Commander of Defense Information Systems Agency's (DISA's) Joint Interoperability Test Command (JITC), Col. Andrew is in a strong position to speak with authority, since he has the responsibility as the DoD's sole certifier of joint interoperability for systems.

"The continued accelerated advancement of information technology ensures that fielded systems do not have the latest and greatest capabilities."

The continued accelerated advancement of information technology ensures that fielded systems do not have the latest and greatest capabilities. The revolution in military affairs is rapidly accelerating the rate at which requirements change, but the essential question should be does the fielded system meet mission requirements?

The revolution in military affairs is built on software. The rapid linking of disparate weapons and command systems is done via software. Therefore, a significant number of interoperability issues are software-based. Laymen commonly think of software in terms of application software. More often than not, interoperability issues dealing with passing targeting data from a sensor platform to a weapons platform (sensor-to-shooter) involve low-level software to include firmware. Firmware is essentially software-reprogrammable chipsets.

Rapid technological advances have also fueled the revolution in business affairs. Innovative solutions are sought to accelerate the fielding of new technology. Commercial off-the-shelf (COTS) software is widely touted as the silver bullet for speeding the delivery of updated software to the field. Unfortunately, there are no COTS products for purely military applications such as embedded weapons systems. Even with application software, some commercial products produce interoperability problems because they are designed to be proprietary closed systems.

Defining the Problem Space

Given the enormous number of C4ISR systems in use in today's armed forces, it is critical that we understand clearly which systems are being addressed by our approach. This section establishes the scope of the problem with which this article will concern itself.

When systems are fielded from outside the DoD acquisition process, interoperability responsibility for these systems is also outside the DoD acquisition commands. In this paper we discuss C4ISR interoperability for systems that have been fielded through project managers (PMs) and program executive officers (PEOs).

Our general approach is to narrow the field to C4ISR systems; ensure that these systems have interoperability requirements; and ensure that we focus on combat requirements. We discuss each of these elements in greater detail, and suggest a methodology for arriving at the "right" list of systems.

What is a C4ISR system? Our approach is concerned with C4ISR systems and may not be applicable to other types of interoperability. The JTA's definition of C4ISR systems is presented in the introduction. C4ISR systems move data that is critical to the conduct of military operations. Information systems that do not move this type of data have no operational requirement to be interoperable. (There may be a functional requirement for reasons of organizational efficiency, but this is distinctly different from an operational requirement.)

The task of identifying all C4ISR systems seems daunting. C4ISR systems are developed by a dizzying array of organizations within the DoD. Fortunately, the preparations for the Year 2000 crisis resulted in extensive efforts throughout the DoD to inventory all computer and communications systems throughout the department. These databases can be leveraged to provide an initial, all-inclusive list of systems. Applying the definition of C4ISR systems provided in the JTA can narrow this list of computer and information systems to those systems that perform C4ISR functions.

The second step is to eliminate problems that are not interoperability problems. Interoperability is defined by the IEEE as "the ability of two or more systems or components to exchange data and use information" (IEEE, 1990). This road map does not apply to deficient capability that is isolated to a particular system. Rather, it focuses on situations in which the ability for multiple systems to communicate, cooperate, or coexist is lacking. At the same time, it is important that we do not construe the potential for interoperability too narrowly — most systems have interaction with other systems at some level. A system should be eliminated at this point only if it meets none of the following criteria:

"The task of identifying all C4ISR systems seems daunting."

- It generates data that is used by another system.
- It processes or consumes data that is generated by another system.
- It relies on another system for delivery of data.
- It is software that operates on the same platform as another system.

For legacy systems, these criteria may narrow the list of systems considerably. However, in today's changing environment, this filter may quickly become less effective. Because of the movement to network-centric systems required by Joint

Visions 2010 and 2020 (JV2010/JV2020), there will be increasing interaction between systems that were previously disjoint. In addition, the proliferation of applications and the need for lighter, more agile components will drive more and more applications away from dedicated computing platforms and onto common ones. This will drive the need for shared service between applications that were previously disjoint.

Finally, we wish to focus on systems that are critical to the unified commands. Problems that do not affect the sharp end of the spear clearly deserve less attention. We are interested in an approach to interoperability that increases the combat capability of the U.S. Armed Forces. Systems that directly impact our ability to accomplish our mission should be the first on our list. We can accomplish this by considering the joint mission essential task lists (JMETLs) of the unified commands. If a particular system does not help to accomplish a JMETL for a unified commander, it can be safely eliminated from consideration.

Thus, we recommend a systematic, three-step methodology. First, each command responsible for C4ISR procurements should identify the universe of all C4ISR systems. Next, eliminate those systems for which interoperability is not an issue. Finally, compare the list to the JMETL of the unified commands, using this to eliminate systems that are either not joint or not mission essential. A diagram describing the process by which we arrive at the final group of systems is shown in Figure 1.

Considering Existing Metrics

Interoperability is notoriously difficult to measure. Although one might at first think that interoperability is an all-or-nothing proposition, this is an oversimplification. For example, systems that can exchange all of the required data elements might be interoperable — but if the speed of the exchange is too slow to support the operational requirements, then the so-called interoperability will not be of operational value. Sometimes interoperability

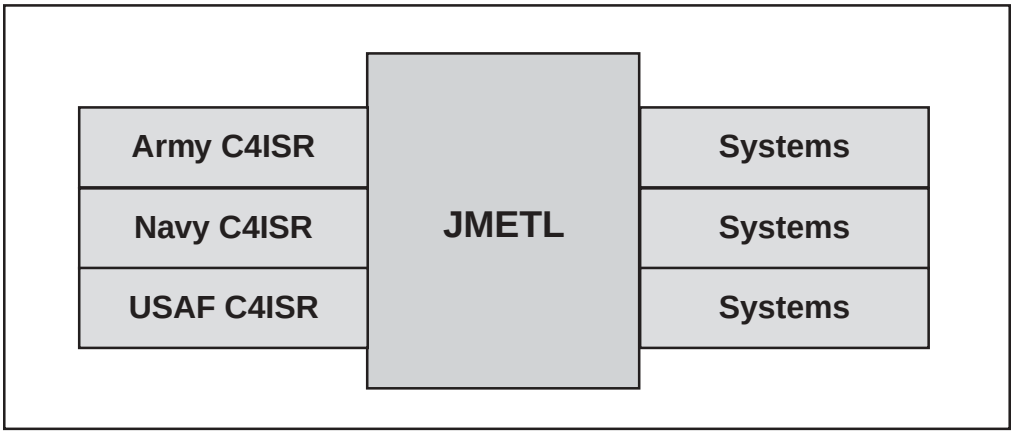

Figure 1. JMETL validated C4ISR Systems from the Service PEO/PM Structure

is realized through labor-intensive workarounds. Are two systems interoperable in this case? It depends on a number of factors: the required frequency; the availability of personnel to operate the workarounds; and, in general, the ability of the procedure to meet the operational requirements (both in terms of effectiveness and suitability).

There has been at least one attempt to measure the interoperability of two systems, through an effort called the Levels of Information System Interoperability (LISI). Rather than a single measure, LISI is actually a collection of related models, a tool for use in applying these models, a set of metrics and techniques for applying the models, and an initiative (or process) aimed at using these models to address a wide set of interoperability objectives. At its core, LISI is based around classifying levels of interoperability by the "richness" of the communication that a particular system or group of systems allows (C4ISR Architecture Working Group, 1998). Although a full discussion of LISI is beyond the scope of this paper, we believe that the model is, at root, too complicated for use in aggregating the status of systems at this level.

A Basis for Measurement

We propose a simplified model, wherein each system will be labeled with a color code based on two factors. The first factor is whether the system has any known interoperability problems. A problem exists if and only if some operational requirement cannot be met because of the deficiency. Some capabilities might be "desirable," but if they are not *required* by the unified commands, then there is no interoperability problem for the purposes of our measure. This first factor, then, measures whether the system meets *operational* requirements. The second factor is whether the system meets its interoperability requirement set. By this we mean that the system has implemented all documented interoperability functionality and has received a joint certification from the JITC. This factor, then, focuses on acquisition requirements. We use this to distinguish between problems of *requirements definition* and problems of *requirements implementation*.

Using these two methods, we arrive at a four-colored system, as described in Tables 1 and 2.

Table 1.
Stop Light Model

		Meets Acquisition Requirements?	
		Yes	No
Meets Operational Requirements?	Yes	Green	Yellow
	No	Orange	Red

Table 2.
Stop Light Color Definition and Implications

Green	The system meets its interoperability requirement set **and** has no known interoperability problems	Fielded system without known issues that meets all documented requirements
Yellow	The system does not meet its interoperability requirement set, **but** has no known interoperability problems	Documented requirements do not reflect operational use of the system
Red	The system does not meet its interoperability requirement set, **but** has no known interoperability problems	Improvement, migration and/or action plans needs to be put in place
Orange	The system meets its interoperability requirement set, **but** has known interoperability problems	Revisit requirements and determine if requirements are adequate

Note that use of the stoplight model involves drawing hard lines between meeting and not meeting requirements. This may not be an entirely straightforward proposition. Nevertheless, the value of drawing a line in the sand between "acceptable" and "unacceptable" cannot be overstated. Only by providing unambiguous judgments on the status of our systems can we move the debate from one of educated guessing (i.e., rumor and innuendo) to one with a degree of rigor and reproducibility.

There is one important point that needs to be made about this grading system. The operational requirements considered should be those that are in force at a particular time. If we are grading a system today, it should be graded with respect to today's operational requirements — if we are projecting a grade for one year from now, it should be based on our best information about next year's operational requirements.

However, the acquisition requirements used should be those that were to have been implemented by a particular point in time. For example, if we have a radio system with a scheduled upgrade, and the requirements process was geared for release of the upgrade in one year, we should not include the upgraded requirements in an evaluation of the system's readiness today. We should, however, include the upgraded requirements in an evaluation of the system's readiness next year — and we should do so using our best information about whether/when the system will meet these requirements. This is important (and fair) because we must recognize that the acquisition community is constrained by technical and fiscal realities, and does not always have the ability to deliver improvements in time. Its schedule is dictated by the ever-present trades with cost and performance, and may even be influenced by the timeliness of the identification of the requirement. This part of

the measurement is designed to measure the acquisition community's ability to respond to the requirements process — and schedule is a key part of that process.

Of course, in both cases, the farther in the future we project these requirements, the more cautiously we must consider their results. Nevertheless, short- and medium-term forecasts are likely to have tremendous planning value. Consider the following notional example illustrated in Figure 2.

System XYZ was fielded one year ago. The original release had some problems with one of its interfaces, and as a result was unable to pass JITC testing. Nevertheless, System XYZ was fielded because it provided significant capability to the Unified Commands. Unfortunately, its failures have limited its operational employment. Therefore, its current interoperability readiness status is red — it has both operational and acquisition problems.

A software fix, just submitted for JITC testing, has undergone favorable initial review and is expected to resolve both the operational and acquisition problems. JITC testing will be completed in three months, so at that time we project that its interoperability readiness status will be

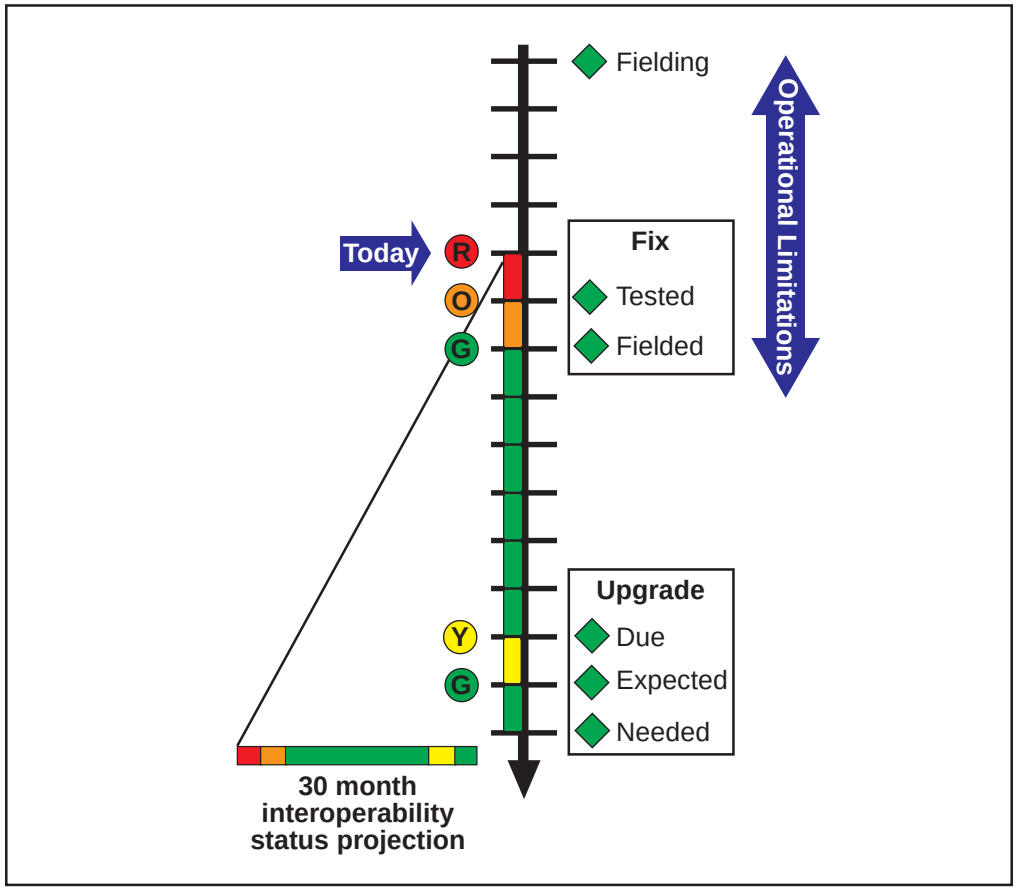

Figure 2. Sample Timeline

orange. Three months later the software fix will be incorporated in all fielded units; so in six months, we project the interoperability readiness status will be green.

Meanwhile, however, System XYZ was fielded with a preplanned product improvement strategy, because the operational requirements were expected to increase dramatically over the course of the next few years. The upgraded system is due in two years, but because the current system implemented a few features early, it will actually continue to function effectively for the next 30 months. As a result of a funding cut, the PM is already warning that the upgrade will be three months late. Therefore, in 24 months we expect the system to enter the yellow state, where it is behind the acquisition cycle but still meets operational requirements. In 27 months when the next version is released, it will become green, and will stay green at 30 months because the system will still meet requirements.

"Instead of grading systems, it may be necessary to unroll this rating and grade the interfaces between systems."

Applying the Basis

The section above describes how each system can be graded using a modified stoplight-style scheme. Systems graded green and yellow meet their operational requirements, although yellow systems warn of possibly overspecified requirements or potential future problems. Systems graded orange and red limit operations. Red systems indicate problems in requirements implementation, whereas orange systems indicate a (potentially harder to solve) problem in requirements definition.

The problem with this scheme is that it may not provide adequate insight into the etiology (root cause) of the problem. Systems with multiple interfaces may be coded red because of problems with only one interface. Instead of grading systems, it may be necessary to unroll this rating and grade the interfaces between systems. Each pair of interacting systems could be given a color code based on the scheme described above.

The advantage to grading interfaces is a more fine-grained understanding of not only the systemic cause of the problem, but also of its operational impact. A red system may perform perfectly well in a large number of operational scenarios, if the most commonly required interfaces are not the causes of the problem. Conversely, it may have little operational value, if the most useful interfaces are the ones with the problem.

The disadvantage to grading interfaces is the dramatic increase in the magnitude of the problem space. With the increased interconnections between systems in the network-centric environment predicted by JV2010, we can expect increasing numbers of interactions between system pairs. Whereas the difficulty of measuring readiness for systems increases with the number of systems, the difficulty of measuring readiness for interfaces increases with the square of the number of systems.

One way to mitigate this problem would be to narrow the number of interfaces considered. Instead of grading all interacting system pairs, it may be useful to begin by evaluating the readiness of each system in

the problem space. For red and orange systems, one might next evaluate each interaction with another system using the readiness reporting model, and then develop remediation plans on a per-interface basis. Once this process was established, yellow systems could be similarly analyzed to determine whether the requirements were overspecified or the systems underutilized, or whether (as in our earlier example) the yellow status was a transient situation that was not cause for great alarm.

Aggregate Measures

Clearly, these readiness measures, by themselves, can provide a useful tool in helping to address the DoD's interoperability efforts. They focus attention first on those systems that do not meet operational requirements, putting emphasis on meeting the warrior's needs. In addition, they help to identify problems in the requirements definition process. By separating problems of implementation from problems of definition, the authors believe the process will highlight the successes of the acquisition community. More important, by identifying problems of definition, they will help to focus efforts in this area, hopefully helping to prevent these problems from recurring in future systems. Given the sometimes long loop between requirements definition and operational employment, it is key that these lessons are fed back into the requirements generation system as quickly as possible so that they are not compounded.

However, it is also important to have a general measure of the overall health of C4ISR interoperability in the DoD. The readiness reporting measures can be used to provide such an aggregate measure.

The simplest way of doing this is to measure the percentage of systems that are classified in each color. Of particular interest would be the percentage of green and yellow systems (the system operational interoperability readiness rate), and the percentage of green and orange systems (the system acquisition interoperability success rate). It might also be interesting to consider the percentage of green and red systems, which indicates the correlation between acquisition success and operational readiness — perhaps providing an indicator of the health of the acquisition process (including the requirements process) as a whole. See Figure 3 for a visual depiction of these rates.

This simple method of aggregating the scores is unambiguous. But does it provide a fair ranking of the interoperability readiness of our C4ISR systems? Because every system has equal weight, a small system filling a relatively small niche in the combat environment (for example, a medical field supply reporting system) is rated equally with a large system that interacts with many other battlefield systems (for example, an AWACS aircraft). This may not be completely appropriate.

"...it is also important to have a general measure of the overall health of C4ISR interoperability in the DoD."

For that reason, it may be desirable to assign weights to each of the systems in our problem domain. This could be done using any number of methods, taking into account factors including, but not limited to, number of interfaces, number of

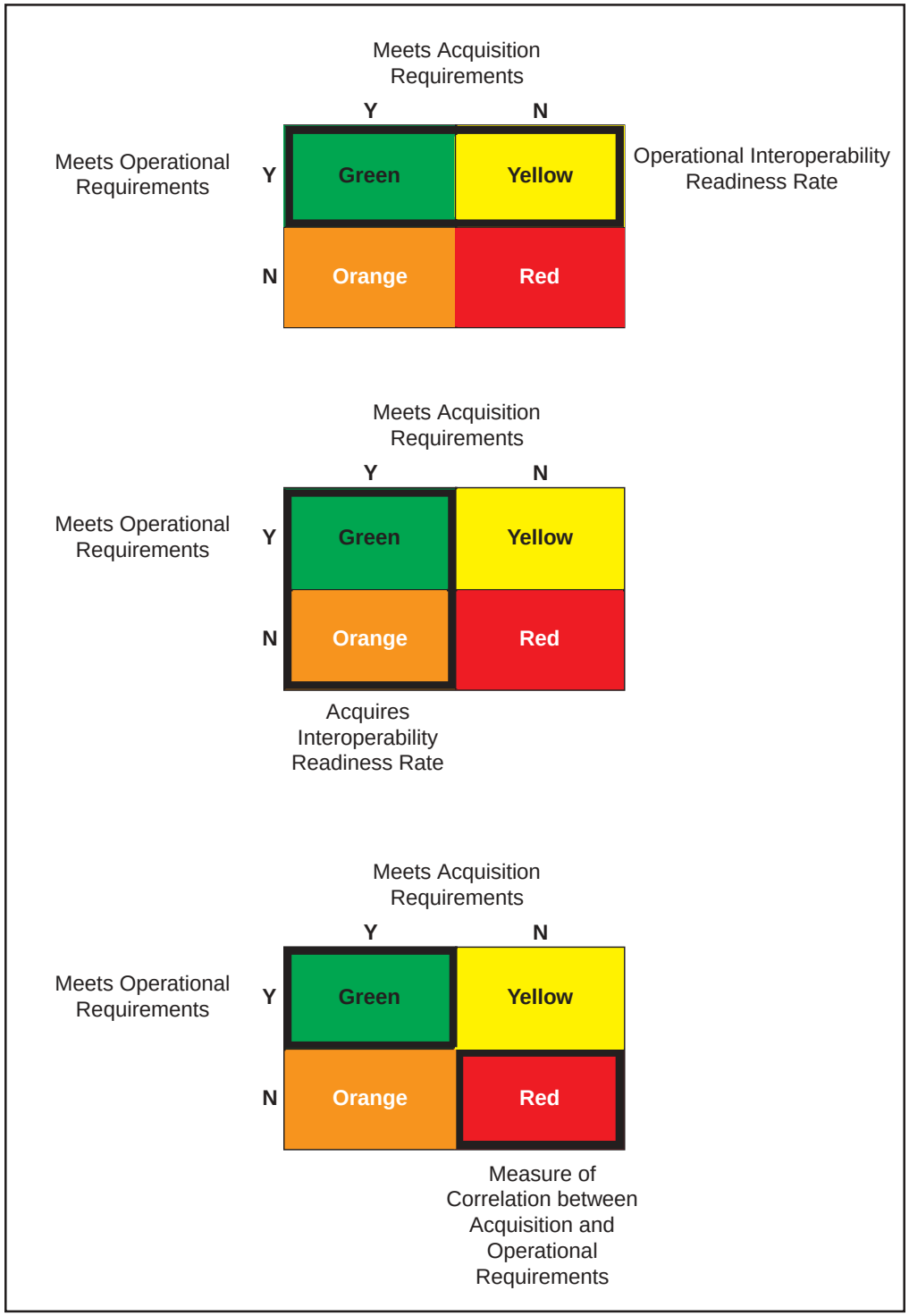

Figure 3. Aggregate Measures

deployed units, or criticality of the system as rated by operational commanders.

The percentages described above could then be calculated with each system contributing a weighted score. (We refer to these measures as weighted system operational interoperability readiness rates, etc.) This might more accurately reflect the state of the department. On the other hand, it might tend to mask problems with relatively small, yet important systems, if the weights are not carefully constructed.

An alternative to using the system readiness indicators would be to use the interface indicators. Again, these could each be given equal weight, or could be weighted based on the importance of the particular interaction between each system pair. We refer to these as interface interoperability readiness rates and weighted interface interoperability readiness rates, respectively.

Clearly, to gain value from these aggregate metrics, they must be maintained. For them to be maintained, the readiness scores for each system (or interface) must be maintained. It is also important to realize that as new systems are fielded, they become legacy systems and must be added to the scoring system.

Perhaps the best way to roll up these figures would be to use them to score the ability of U.S. forces to meet various mission scenarios. By developing notional architectures for operational employment of our forces, the interoperability readiness reporting measures could be used in the same way existing readiness measures are used. In this case, typically, the lowest score would dominate and be carried up to a higher level. This would provide valuable insight into the ability of C4ISR systems to meet national strategic needs, and would help to justify funds for improvements where they are required.

Discussion: Solving the Problem

With this collection of metrics we can now propose a road map for a department wide approach to addressing the C4ISR interoperability problem. First, identify an agency with responsibility for overseeing the road map. Second, under the direction of the lead agency, develop an authoritative list of systems that fall into the problem space identified in this paper, together with an institutionalized process for maintaining that list. Third, develop readiness scores (and, possibly, weights) for each system on the list, together with an institutionalized process for maintaining this data. Fourth, using the first consolidated, across-the-board data set, measure the current state of our legacy C4ISR interoperability problem. Finally, set realistic goals for improving this state, allocating the resources required to realize those goals, and measuring progress along the way. This section will discuss this approach in more detail.

"...we can now propose a road map for a department wide approach to addressing the C4ISR interoperability problem."

The issues surrounding C4ISR interoperability affect the services, defense agencies, and the unified acquisition community. In addition, success in this effort ultimately requires the ability to prioritize problems across the military community and to allocate resources in support of the priorities. The authors believe that this

function is fundamentally related to Joint Forces Command's UCP-99 responsibilities as joint forces trainer, provider, and integrator, and that application of this metric is consistent with and supportive of their other objectives.

As its first task, the lead office would need to compile a master list of mission essential C4ISR systems with interoperability requirements. An approach for doing this is outlined in the first section of the paper. Just as important as compiling the initial list, the organization must put in place a process for maintaining the list, involving all of the various entities throughout the DoD that field C4ISR systems. This encompasses a large array of organizations, including Communications and Electronics Command (CECOM), Space and Warfare Systems Command (SPAWAR), Electronic Systems Command (ESC), Naval Air Systems Command (NAVAIR), Naval Sea Systems Command (NAVSEA), and PEOs within the Air Force and Army, DISA, Defense Intelligence Agency (DIA), National Security Agency (NSA), Special Operations Command (SOCOM), and others. This process would most likely involve integration of existing processes, rather than development of new ones; nevertheless, given the number of developing organizations, this represents a potentially nontrivial effort. Even by itself, however, this task will likely result in a valuable resource by identifying all systems in this class, together with the responsible agency.

"Once again, determining the status of these systems is not enough."

With the master list in hand, this office could then begin to assess the readiness of each of these systems. This rating need not be done by a single office, but could be delegated to subordinate agencies. The key to this evaluation, in fact, is to ensure that the operational community evaluates the operational requirements, while the acquisition community evaluates the acquisition requirements. The office, of course, would be responsible for providing sufficient oversight to ensure honest responses were provided. In addition to understanding "today's" situation, data should be collected on the projected status over the medium term, perhaps 3–5 years. As described in the example earlier, changes in status can sometimes be predicted in advance, and knowing when these changes will take place is important data for decision makers.

Once again, determining the status of these systems is not enough. The office must put in place procedures for maintaining this information. The challenge here comes from the large number of players. Although much of this information exists within the department, making it accessible in normalized form in a centralized location would represent a key contribution to dealing with the interoperability problem.

Once the list of systems and the data on each system is available, and an institutional process for maintaining it is in place, the office's work becomes at once simpler and more significant. In addition to keeping the process running (which is likely to remain nontrivial in light of the propensity for reorganization within the federal government), the office must compile aggregate statistics (including projections of the aggregate statistics). More

important, the office must drill down into the interfaces of problem systems, determining the true sources of problems, and engage the necessary players to effect solutions. This could be done both to solve present problems and to prevent or mitigate problems that may be anticipated.

Of course, in addition to the department-wide statistics, the data could be cut along different lines. One could consider the interoperability readiness of all sensors, all shooters, all systems within a particular area of interest, or all systems produced by a particular agency. Using interface data, one could even construct a picture of the "interoperability" between two agencies by considering the status of interfaces for systems produced by the two agencies. This might identify instances in which institutional obstacles played a role in the observed interoperability problems. Equally important, it would likely highlight the tremendous levels of cooperation between many of the agencies acquiring C4ISR systems.

Armed with hard data, "ground truth" can be provided to the interoperability debate. Realistic goals could be set, and the resources to achieve these goals could be allocated to the organizations in the best positions to do so. Most important, progress toward these goals could be objectively measured. The process would separate requirements issues from acquisition issues, offering opportunities for improving both of these systems when systemic factors are found to have contributed to problems. At the same time, it would ideally protect all parties from recrimination by focusing the entire community on solving the problem — delivering C4ISR systems that meet the interoperability demands of our warriors.

Conclusion

One can easily argue that America's unrivalled dominance on the battlefields of the late 20th century is due largely to the success of our acquisition system, even in light of the declining defense budgets of the last decade.

Our ability to attain full-spectrum dominance in the 21st century will rely heavily on our C4ISR infrastructure (Chairman of the Joint Chiefs of Staff, 2000). Interoperability of our C4ISR systems is essential to achieving this goal. We are doing well in this area, but we can do better.

That which is measured improves. We will never fully eliminate interoperability problems, because evolving operational requirements will continue to challenge the developers of C4ISR systems. By its very nature, our enterprise will always be pushing the limits of technology, generating new problems even as the old ones are solved. It is important to show progress, analyze the drivers behind our interoperability problems, and apply maximum effort at the point of greatest leverage to solve them. Only in this way can we provide the greatest possible utility to the soldier on the battlefield.

We have developed a simple, readiness-reporting style method of measuring interoperability. We also have proposed a method for aggregating the data in a manner that will facilitate tracking progress on a DoD-wide basis. Finally, we have outlined a mechanism for applying the metrics within the DoD to facilitate solution of the problem. It is our sincere hope that this road map will generate open discussion within the department that will ultimately lead to a more rigorous approach to interoperability.

Lieutenant Colonel John A. Hamilton, Jr., USA, is director of the Joint Forces Program Office. His 20-year career in the U.S. Army has included assignments as research director and assistant professor at the U.S. Military Academy, director of the Ada Joint Program Office, and a chief of both the Officer Training Division and the Software Engineering Branch of the Computer Science School at Fort Gordon, GA. Hamilton has been published widely at conferences and in refereed journals and is the coauthor of a book, *Distributed Simulation*. He earned a B.A. in journalism/public relations from Texas Tech University, an MS in management information systems from the University of Southern California, an MS in computer science from Vanderbilt University, and a Ph.D. in computer science from Texas A&M University.

(E-mail address: hamiltoj@spawar.navy.mil)

Major Paul A. Summers, USAF, is the deputy director of the Joint Forces Program Office. He previously worked as a requirements officer at the U.S. Air Force Space Command Directorate of Requirements and as team lead for the development of the Combat Survivor Evader Locator radio program. Summers earned a B.S. degree in aerospace engineering from the University of Colorado and an M.S. in acquisition logistics management from the U.S. Air Force Institute of Technology.

(E-mail address: summersp@spawar.navy.mil)

Captain J. David Rosen, USAF, is currently an interoperability project engineer at the Joint Forces Program Office, a new San Diego-based organization addressing warfighter interoperability concerns at the service's Command and Control (C2) system commands. Rosen previously served as an information system security engineer in the National Security Agency's Information System Security Organization. He earned a B.S. degree in computer engineering, a B.S. in mathematics/computer science, and an M.S. in electrical and computer engineering from Carnegie Mellon University.

(E-mail address: rosenj@spawar.navy.mil)

References

C4ISR Architecture Working Group. (1998). *Levels of information system interoperability (LISI)*. Place of publication: Publisher.

Communications Architecture Working Group. (1998). C4ISR Working Group. *Levels of Information systems interoperability (LISI)*. Retrieved from http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdfdocs/lisi.pdf.

Defense Information Systems Agency. (1999). *Joint technical architecture, v. 3.0, draft 1*. Arlington, VA: Author.

IEEE. (1990). IEEE standard 610.12-1990. In *IEEE standard glossary of software engineering terminology* (p. 42). Piscataway, NJ: Author.

Chairman of the Joint Chiefs of Staff. (2000). *Joint vision 2020*. Washington, DC: U.S. Government Printing Office.